Issue Number : 5-5-2007-025771731

대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2007-0038466
Application Number

출 원 년 월 일 : 2007년 04월 19일
Filing Date APR 19, 2007

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Institute

2007년 05월 09일

특 허 청
COMMISSIONER

◆ This certificate was issued by Korean Intellectual Property Office. Please confirm any forgery or alteration of the contents by an issue number or a barcode of the document below through the KIPOnet- Online Issue of the Certificates' menu of Korean Intellectual Property Office homepage (www.kipo.go.kr). But please notice that the confirmation by the issue number is available only for 90 days.

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2007.04.19

【발명의 국문명칭】 악성 코드가 숨겨진 파일 탐지 장치 및 방법

【발명의 영문명칭】 Detection Apparatus and Method of Embedded Malicious Code in File

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【대리인】

【성명】 권태복

【대리인코드】 9-2001-000347-1

【포괄위임등록번호】 2001-057650-1

【대리인】

【성명】 이화익

【대리인코드】 9-1998-000417-9

【포괄위임등록번호】 1999-021997-1

【발명자】

【성명】 김윤주

【성명의 영문표기】 KIM Yun Ju

【주민등록번호】 801124-2XXXXXXX

【우편번호】 443-400

【주소】 경기 수원시 영통구 망포동 극동아파트 101동 102호

【국적】 KR

【발명자】

【성명】 윤영태

【성명의 영문표기】 YUN Young Tae

【주민등록번호】 710125-1XXXXXXX

【우편번호】 301-780

【주소】 대전 중구 태평2동 버드내아파트 206동 202호

【국적】 KR

【우선권 주장】

【출원국명】 KR

【출원종류】 특허

【출원번호】 10-2006-0111853

【출원일자】 2006.11.13

【증명서류】 첨부

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 심사청구를 합니다.

대리인 권태복 (인)

대리인 이화익 (인)

【수수료】

【기본출원료】	0 면	38,000 원
【가산출원료】	19 면	0 원
【우선권주장료】	1 건	20,000 원
【심사청구료】	11 항	461,000 원
【합계】	519,000 원	
【감면사유】	정부출연연구기관	
【감면후 수수료】	269,500 원	

【기술이전】

【기술양도】 희망

【실시권허여】 희망

【기술지도】 희망

【요약서】

【요약】

본 발명은 파일 처리 과정에서 동작하는 프로세스에 대해 비정상 유무를 확인하여 악성 코드가 숨겨진 파일을 탐지하는 장치 및 방법에 관한 것으로, 그 구성은 검사대상파일에 실행 파일 포맷이 포함되어 있는지 정적분석(static analysis) 통해 탐색하는 실행코드 탐지모듈과, 상기 검사대상파일의 확장자에 따라 지원프로그램을 검색하여 해당하는 프로세스명과 실행 경로를 알려주는 지원프로그램 검색모듈과, 상기 검색한 지원프로세스를 모니터링하여 새로 생성되는 프로세스에 대한 부모 프로세스의 정상유무를 프로세스의 트리(tree)구조를 이용해 판단하는 비정상 프로세스 탐지모듈과, 상기 검사대상파일이 악성 파일로 판단되면 상기 새로 생성되는 프로세스를 강제 종료하는 비정상프로세스 강제종료모듈을 포함함으로써 모든 비정상적인 프로세스의 실행을 원천적으로 막아낼 수 있다.

【대표도】

도 1

【색인어】

악성 코드, 오피스 문서

【명세서】

【발명의 명칭】

악성 코드가 숨겨진 파일 탐지 장치 및 방법{Detection Apparatus and Method of Embedded Malicious Code in File}

【도면의 간단한 설명】

<1> 도 1은 본 발명에 따른 악성 코드가 숨겨진 파일 탐지 장치의 전체 구성도,

<2> 도 2는 본 발명에 따른 악성 코드가 숨겨진 파일 탐지 방법을 나타낸 순서도이다.

<3> <도면의 주요 부호에 대한 설명>

<4> 10. 사용자 인터페이스 101. 실행코드 탐지모듈

<5> 102. 지원프로그램 검색모듈 103. 비정상프로세스 탐지모듈

<6> 104. 정상프로세스 DB 105. 비정상프로세스 강제종료모듈

<7> 106. 디스플레이부

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<8> 본 발명은 특정 프로그램에서 지원하는 파일 형식(doc, ppt, xls, hwp, wmf 등)을 처리하는 과정에서의 취약점을 이용해 임의의 실행 파일 포맷을 실행하는 악성 코드가 숨겨진 파일을 탐지하는 방법에 관한 것으로, 더욱 상세하게는 파일 처리 과정에서 동작하는 프로세스에 대해 비정상 유무를 확인하여 악성 코드가 숨겨진 파일을 탐지하는 장치 및 방법에 관한 것이다.

<9> 최근 doc-MS Office Word, ppt-MS Office PowerPoint, xls-MS Office Excel, hwp-한글, wmf-MS Windows Media Player와 같이 특정 확장자를 지원하는 프로그램의 취약점을 이용하여 파일에 숨겨진 임의의 코드를 실행하는 기법으로 많은 공격이 이루어지고 있다.

<10> 이 기법은 악성 코드가 숨겨진 파일을 이메일, 메신저, P2P 등으로 전파되었을 때, 사용자가 파일을 해당 프로그램으로 실행하기만 하면 악성 코드가 실행되기 때문에 일반 사용자로서는 알기 어려운 위협일뿐만 아니라 그 영향력도 상당하다.

<11> 이러한 기법의 공격중 MS Office 제품군을 이용한 공격을 탐지하는 방법으로 국내특허출원 10-2005-0044241호 "악성 코드가 숨겨진 오피스 문서 탐지 방법"이 있다. 이 특허는 일반적으로 많이 사용되는 마이크로소프트 제품군의 오피스 문서

의 매크로 기능을 이용하여 숨겨진 악성코드를 실행하는 취약점을 사용한 악성코드 탐지가 현재 국내 및 외산 백신에서 불가능하기 때문에 이를 탐지하는 방법을 제시하였다.

<12> 이처럼 종래기술들은 오직 매크로만을 이용하여 특정 악성코드를 실행시키는 공격에 대한 대응이거나 이미 알려진 패턴 매칭에 의한 악성 코드를 탐지하는 기술이었다.

<13> 그러나 이러한 방법은 숨겨진 악성코드가 인코딩되어 있고, 매크로를 이용하여 임의의 코드를 실행하는 취약점을 사용한 것이 아닌 경우에 탐지가 불가능한 문제가 있다.

【발명이 이루고자 하는 기술적 과제】

<14> 상기한 종래 기술의 문제점을 해결하기 위한 본 발명의 목적은 단순히 매크로뿐만 아니라 모든 프로그램들이 자신이 지원하는 파일 형식을 처리하는 과정에서의 취약점을 이용한 공격에 대응할 수 있고, 기본적인 패턴 매칭 기법이 아닌 파일 처리 과정에서 동작하는 모든 비정상적인 프로세스의 실행을 원천적으로 막아낼 수 있는 악성 코드가 숨겨진 파일 탐지 장치 및 그 방법에 관한 것이다.

【발명의 구성】

<15> 본 발명에 따른 악성 코드가 숨겨진 파일 탐지 장치는 검사대상파일에 실행 파일 포맷이 포함되어 있는지 정적분석(static analysis)을 통해 탐색하는 실행코드 탐지모듈과, 상기 검사대상파일의 확장자에 따라 지원프로그램을 검색하여 해당하는 프로세스명과 실행 경로를 알려주는 지원프로그램 검색모듈과, 상기 검색한 지원프로세스를 모니터링하여 생성되는 새로운 프로세스에 대한 부모 프로세스의 정상유무를 프로세스의 트리(tree)구조를 이용해 판단하는 비정상프로세스 탐지모듈과, 상기 검사대상파일이 악성 파일로 판단되면 상기 생성되는 새로운 프로세스를 강제 종료하는 비정상프로세스 강제종료모듈을 포함하여 구성되는 것을 특징으로 한다.

<16> 한편, 본 발명에 따른 악성 코드가 숨겨진 파일 탐지 방법은 검사대상파일에 실행 파일 포맷이 존재하는지를 판단하기 위해 정적분석(static analysis)을 수행하는 1단계와, 상기 정적분석 결과, 상기 검사대상파일에 실행 파일 포맷 MZ header 및 PE header가 존재하지 않는 경우에는 상기 검사대상파일의 지원프로그램을 실행하여 새로운 프로세스의 생성 여부를 모니터링하는 2단계와, 상기 모니터링 결과에 따라 상기 검사대상파일에 대한 상기 새로운 프로세스의 정상 유무를 판단하는 3단계를 포함하여 이루어지는 것을 특징으로 한다.

<17> 또한, 상기 악성 코드가 숨겨진 파일 탐지 방법은 상기 3단계에서 상기 새로운 프로세스가 비정상 프로세스로 판단되면 상기 검사대상파일이 악성 파일로 판단하여 상기 새로운 프로세스를 강제종료하는 4단계를 더 포함하여 이루어지는 것을 특징으로 한다.

<18> 또한, 상기 2단계는 상기 검사대상파일을 지원하는 지원프로그램을 검색하는 2-1단계와, 상기 지원프로그램으로 상기 검사대상파일을 실행하는 2-2단계와, 상기 지원프로그램의 실행에서 새로운 프로세스가 생성되는지 모니터링하는 2-3단계를 포함하여 이루어지는 것을 특징으로 한다.

<19> 또한, 상기 3단계는, 상기 2단계의 모니터링 결과, 상기 생성된 새로운 프로세스의 부모 프로세스가 지원프로그램의 프로세스인지 프로세스의 트리(tree)구조를 이용해 확인하는 3-1단계와, 부모 프로세스가 지원프로그램이면 정상 프로세스 DB에 상기 생성된 새로운 프로세스명이 있는지 검색하는 3-2단계와, 상기 검색결과, 상기 정상 프로세스 DB에 상기 생성된 새로운 프로세스명이 없으면 비정상프로세스로 판단하는 3-3단계를 포함하여 이루어지는 것을 특징으로 한다.

<20> 이하 본 발명의 악성 코드가 숨겨진 파일 탐지 장치(100)에 대하여 도 1을 참조하여 상세하게 설명한다.

<21> 도 1은 본 발명에 따른 악성 코드가 숨겨진 파일 탐지 장치(100)의 구성을 나타낸 것으로서, 악성 코드가 숨겨진 파일 탐지 장치(100)는 실행코드 탐지모듈(101), 지원프로그램 검색모듈(102), 비정상프로세스 탐지모듈(103), 정상프로세스 DB(104), 비정상프로세스 강제종료모듈(105) 및 디스플레이부(106)를 포함한다.

<22> 본 발명에 따르면, 악성 코드가 숨겨진 파일 탐지 장치(100)는 사용자 인터페이스(user interface)(10)를 통해 사용자로부터 검사대상파일을 입력받고, 입력받은 검사대상파일에 악성 코드가 포함되어 있는지를 검사하고, 그 검사 결과를 출력한다.

<23> 구체적으로, 본 발명의 악성 코드가 숨겨진 파일 탐지 장치(100)의 실행코드 탐지모듈(101)은 사용자 인터페이스(user interface)(10)를 통해 입력받은 검사대상파일에 정적분석(static analysis)을 수행하여 실행 파일 포맷인 MZ Header와 PE Header가 포함되어 있는지 탐지한다.

<24> 탐지 결과, 검사대상파일에 실행 파일 포맷인 MZ Header와 PE Header가 포함되어 있으면, 검사대상파일을 악성 코드가 숨겨진 파일, 즉 악성 파일로 판단하고, 포함되어 있지 않으면 검사대상파일을 실행할 수 있는 지원프로그램을 검색하도록

한다.

<25> 상세하게는 실행코드 탐지모듈(101)은 검사대상파일에 대해 실행 가능한 파일 포맷을 찾아 해당 문자열이 일반 PE 파일 구조에 맞는 PE 포맷 규정에 따르며, 또한 실행 가능한지 DOS MZ header - PE header 부분까지 검사하여 위 두 가지 조건에 맞는 경우 해당 파일에 대해 악성 코드가 임베이드(embadded)된 것으로 탐지한다.

<26> 여기서, PE는 Portable Executable(이식가능한 실행 프로그램)를 뜻하며, Win32의 기본적인 파일 형식이다. "Portable Executable"의 의미는 win32 플랫폼 하에서 공통으로 사용할 수 있음을 뜻한다. 모든 Win32 실행파일(VxD와 16비트 DLL 제외)은 PE 파일형식을 사용한다.

<27> 한편 검사대상파일에서 악성 코드가 탐지되지 않는 경우에는 검사대상파일 형식을 지원하는 프로그램을 검색한다.

<28> 지원프로그램 검색모듈(102)은 검사대상파일의 확장자에 해당하는 지원 프로그램을 검색하여 해당하는 프로세스명과 실행경로를 알려준다. 예를 들면, 검사대상파일의 확장자가 doc이면 지원프로그램을 검색하였을 때, 그 결과인 MS Office

Word의 프로세스명과 실행 경로를 알려준다.

<29> 비정상프로세스 탐지모듈(103)은 검사대상파일을 실행하는 프로세스를 모니터링하여 생성되는 새로운 프로세스의 부모 프로세스가 지원프로그램이면서 정상 프로세스에 해당하는지 정상 프로세스 DB(104)를 검색하여 비교한다.

<30> 여기서, 정상 프로세스 DB(104)에는 프로그램에서 정상적으로 생성하는 프로세스를 미리 정의하여 저장한다.

<31> 검색 결과, 부모 프로세스가 정상 프로세스 DB(104)에서 검색되지 않으면 새로운 프로세스가 비정상프로세스이므로 검사대상파일을 악성 파일로 판단하고, 검색되면, 정상 프로세스이므로 검사대상파일을 정상 파일로 판단한 후 이러한 결과를 디스플레이부(106)를 통해 출력한다.

<32> 비정상프로세스 탐지모듈(103)의 비정상프로세스의 판단은 Win32에서 모든 프로세스는 트리(tree) 구조로 이루어져 있기 때문에 각각의 부모(parent) 프로세스와 자식(child) 프로세스의 관계를 통해 비정상프로세스로 예상되는 프로세스를 판단한다. 따라서 검사대상파일 형식을 지원하는 프로그램을 실행하는 과정에서 비정상적인 프로세스를 생성하면 악성 파일로 판단한다.

<33> 비정상프로세스 강제종료모듈(105)은 검사대상파일이 악성 파일로 판단되었을 때, 생성된 새로운 프로세스를 강제 종료하고, 검사대상파일이 악성 파일임을 디스플레이부(106)를 통해 출력한다.

<34> 그러면 상술한 바와 같은 악성 코드가 숨겨진 파일 탐지 장치(100)에서 악성 코드가 숨겨진 파일을 탐지하는 과정에 대해 도 2를 참조하여 상세하게 설명한다.

<35> 도 2는 본 발명에 따라 악성 코드가 숨겨진 파일, 즉 악성 파일을 탐지하는 과정을 도시한 흐름도이며 다음과 같은 각 단계로 수행된다.

<36> 사용자에 의해 장치 및 프로그램이 시작되고(201), 사용자 인터페이스(10)를 통해 사용자가 검사대상파일을 입력하면(202), 실행코드 탐지모듈(101)은 정적분석(static analysis)을 통해 검사대상파일 내부에 MZ Header가 존재하는지 검사한다(203).

<37> 검사결과(203), 검사대상파일 내부에 MZ Header가 존재하면 PE Header가 존재하는지 검사한다(204). 검사대상파일 내부에 PE Header가 존재하면, 검사대상파일을 악성 코드가 숨겨진 파일로 판단(205)하여 결과를 출력(215)하고, 장치 및 프로그램을 종료한다(216).

<38> 검사결과(203), 검사대상파일 내부에 MZ Header가 존재하지 않으면 지원프로그램 검색모듈(102)에서 검사대상파일을 지원하는 지원프로그램을 검색한다(206). 비정상프로세스 탐지모듈(103)에서 지원프로그램에 대한 프로세스 모니터링을 시작(207)하여 검색한 지원프로그램으로 검사대상파일을 실행한다(208).

<39> 프로세스 모니터링(207) 중 새로운 프로세스가 생성되었는지 확인(209)하고, 확인결과(209), 새로운 프로세스가 생성되면 프로세스의 트리(tree)구조를 이용하여 생성된 프로세스의 부모 프로세스가 지원 프로그램의 프로세스인지 확인(210)한다.

<40> 확인결과(210), 생성된 프로세스의 부모 프로세스가 지원 프로그램의 프로세스이면, 생성된 새로운 프로세스명이 정상 프로세스 DB(104)에 존재하는지 검색한다(211).

<41> 검색결과(211), 새로 생성된 프로세스명이 정상 프로세스 DB(104)에 존재하지 않으면 악성파일로 판단(212)하여 비정상프로세스 강제종료모듈(105)에서 비정상 프로세스인 새로운 프로세스를 강제종료하고(213), 검사대상파일이 악성 파일임을 출력(215)한 후 장치 및 프로그램을 종료한다(216). 그렇지 않으면, 지원프로그

램이 끝날 때까지 프로세스 모니터링(209)을 반복한다.

<42> 만약, 확인결과(209), 지원프로그램이 종료할 때까지 새로운 프로세스를 생성하지 않았거나, 검색결과(211) 생성된 새로운 프로세스가 정상이면 정상파일로 판단하여 결과를 출력(215)하고, 장치 및 프로그램을 종료한다(216).

<43> 이상에서 몇 가지 실시예를 들어 본 발명을 더욱 상세하게 설명하였으나, 본 발명은 반드시 이러한 실시예로 국한되는 것이 아니고 본 발명의 기술사상을 벗어나지 않는 범위 내에서 다양하게 변형실시될 수 있다.

【발명의 효과】

<44> 상술한 바와 같이 본 발명에 의한 악성 코드가 숨겨진 파일 탐지 장치 및 방법은 실행 파일뿐만 아니라 하위 프로세스 실행 여부에 따른 비정상프로세스 생성을 이용하여 탐지함으로써 악성코드가 숨겨진 파일에 대해서 알려지지 않은 악성코드를 탐지할 수 있으며, 또한, 특정 프로그램에서 지원하는 파일 형식을 처리하는 과정에서의 취약점을 이용하는 악서 파일을 모두 탐지할 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

검사대상파일에 실행 파일 포맷이 포함되어 있는지 정적분석(static analysis)통해 탐색하는 실행코드 탐지모듈;

상기 검사대상파일의 확장자에 따라 지원프로그램을 검색하여 해당하는 프로세스명과 실행 경로를 알려주는 지원프로그램 검색모듈;

상기 검색한 지원프로세스를 모니터링하여 생성되는 새로운 프로세스에 대한 부모 프로세스의 정상유무를 프로세스의 트리(tree)구조를 이용해 판단하는 비정상 프로세스 탐지모듈; 및

상기 검사대상파일이 악성 코드가 숨겨진 파일로 판단되면 상기 생성되는 새로운 프로세스를 강제 종료하는 비정상프로세스 강제종료모듈

을 포함하여 구성되는 것을 특징으로 악성 코드가 숨겨진 파일 탐지 장치.

【청구항 2】

제1항에 있어서,

상기 실행코드 탐지모듈은 상기 정적분석(static analysis)을 통해 상기 검사대상파일에 실행 파일 포맷 MZ header 및 PE header가 존재하는지를 탐색하는 것을 특징으로 악성 코드가 숨겨진 파일 탐지 장치.

【청구항 3】

제1항 또는 제2항에 있어서,

상기 비정상프로세스 탐지모듈은 상기 새로 생성되는 프로세스의 부모 프로세스의 정상유무를 정상 프로세스 DB에 프로세스명이 존재하는지 여부에 의해 판단하는 것을 특징으로 하는 악성 코드가 숨겨진 파일 탐지 장치.

【청구항 4】

제1항에 있어서,

상기 비정상프로세스 강제종료모듈은 상기 비정상프로세스 탐지모듈에서 상기 생성되는 새로운 프로세스에 대한 부모 프로세스가 비정상프로세스로 판단되면, 상기 검사대상파일을 악성 코드가 숨겨진 파일로 판단하여 상기 생성되는 새로운 프로세스를 강제 종료하는 것을 특징으로 하는 악성 코드가 숨겨진 파일 탐지 장치.

【청구항 5】

검사대상파일에 실행 파일 포맷이 존재하는지를 판단하기 위해 정적분석(static analysis)을 수행하는 1단계;

상기 정적분석 결과, 상기 검사대상파일에 실행 파일 포맷 MZ header 및 PE header가 존재하지 않는 경우에는 상기 검사대상파일의 지원프로그램을 실행하여 새로운 프로세스의 생성 여부를 모니터링하는 2단계; 및

상기 모니터링 결과에 따라 상기 검사대상파일에 대한 상기 새로운 프로세스의 정상 유무를 판단하는 3단계

를 포함하여 이루어지는 것을 특징으로 하는 악성 코드가 숨겨진 파일 탐지

방법.

【청구항 6】

제5항에 있어서,

상기 정적분석은 상기 검사대상파일에 실행 파일 포맷 MZ header 및 PE header가 존재하는지 검사하는 것에 의해 수행되는 것을 특징으로 하는 악성 코드가 숨겨진 파일 탐지 방법.

【청구항 7】

제6항에 있어서,

상기 정적분석 결과, 상기 검사대상파일에 실행 파일 포맷 MZ header 및 PE header가 존재하는 경우에는 상기 검사대상파일을 악성 코드를 포함한 파일로 판단하여 결과를 출력한 후 종료하는 것을 특징으로 하는 악성 코드가 숨겨진 파일 탐지 방법.

【청구항 8】

제5항에 있어서,

상기 2단계는 검사대상파일의 확장자를 이용하여 상기 검사대상파일을 지원하는 지원프로그램을 검색하는 2-1단계;

상기 지원프로그램으로 상기 검사대상파일을 실행하는 2-2단계; 및

상기 지원프로그램의 실행에서 새로운 프로세스가 생성되는지 모니터링하는 2-3단계

를 포함하여 이루어지는 것을 특징으로 하는 악성 코드가 숨겨진 파일 탐지 방법.

【청구항 9】

제5항에 있어서,

상기 3단계는, 상기 2단계의 모니터링 결과, 상기 생성된 새로운 프로세스의 부모 프로세스가 지원프로그램의 프로세스인지 프로세스의 트리(tree)구조를 이용해 확인하는 3-1단계;

부모 프로세스가 지원프로그램이면 정상 프로세스 DB에 상기 생성된 새로운 프로세스명이 있는지 검색하는 3-2단계; 및

상기 검색결과, 상기 정상 프로세스 DB에 상기 생성된 새로운 프로세스명이 없으면 비정상프로세스로 판단하는 3-3단계

를 포함하여 이루어지는 것을 특징으로 하는 악성 코드가 숨겨진 파일 탐지 방법.

【청구항 10】

제9항에 있어서

상기 3단계는 상기 2단계의 모니터링 결과, 상기 생성된 새로운 프로세스의 부모 프로세스가 정상 프로세스 DB에 있으면 정상 프로세스로 판단하여 상기 검사대상파일을 정상 파일임을 출력한 후 종료하는 것을 특징으로 하는 악성 코드가 숨

겨진 파일 탐지 방법.

【청구항 11】

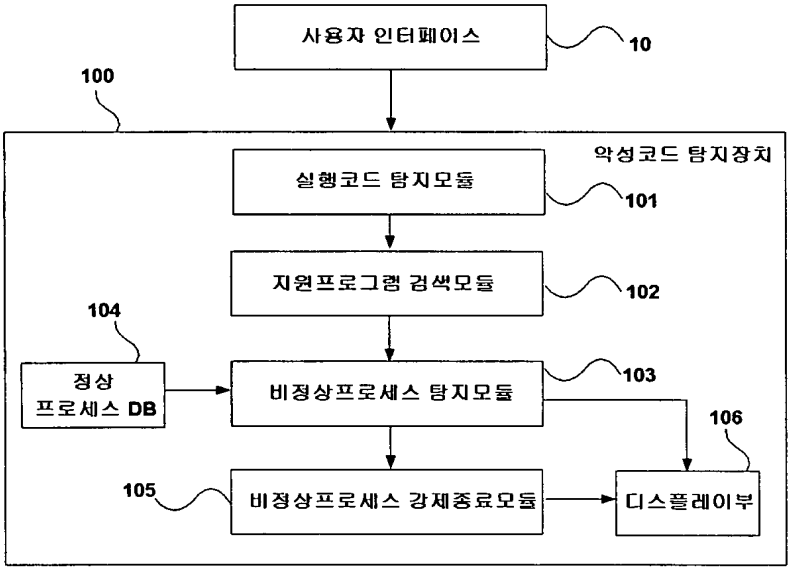
제5항에 있어서,

상기 악성 코드가 숨겨진 파일 탐지 방법은 상기 3단계에서 상기 새로운 프로세스가 비정상 프로세스로 판단되면 상기 검사대상파일이 악성 파일로 판단하여 상기 새로운 프로세스를 강제종료하는 4단계

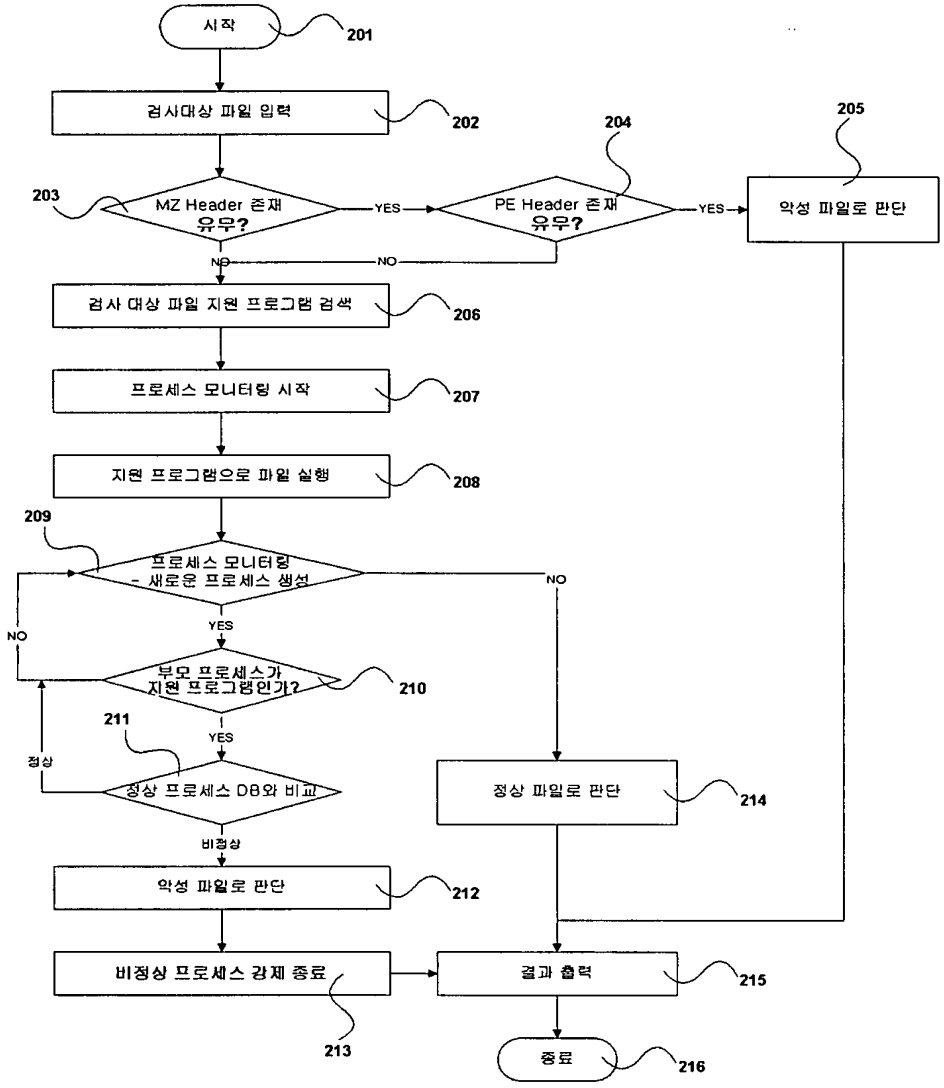
를 더 포함하여 이루어지는 것을 특징으로 하는 악성 코드가 숨겨진 파일 탐지 방법.

【도면】

【도 1】


사용자 인터페이스
10
100
악성코드 탐지장치
실행코드 탐지모듈
101
지원프로그램 검색모듈
102
104
정상
프로세스 DB
비정상프로세스 탐지모듈
103
106
105
비정상프로세스 강제종료모듈
디스플레이부

【도 2】


시작
201
검사대상 파일 입력
202
MZ Header 존재 유무?
203
YES
PE Header 존재 유무?
204
YES
악성 파일로 판단
205
NO
NO
검사 대상 파일 지원 프로그램 검색
206
프로세스 모니터링 시작
207
지원 프로그램으로 파일 실행
208
209
프로세스 모니터링 - 새로운 프로세스 생성
NO
YES
NO
부모 프로세스가 지원 프로그램인가?
210
YES
211
정상
정상 프로세스 DB와 비교
정상 파일로 판단
214
비정상
악성 파일로 판단
212
비정상 프로세스 강제 종료
213
결과 출력
215
종료
216